

Quantum Information and Computing

Ervin Kafexhiu

University of Tirana, Faculty of Natural Sciences

22 May 2025

Motivation

Motivation

- Computers play a fundamental role in society (Science, Industry, Finance, AI etc.)
- More data available \Rightarrow **More computational power needed!**
- We are reaching physical limits of classical hardware!
- So called Moore's law, may not be valid in the future.
- New alternatives are explored.
- We are close to a **Second Quantum Revolution**. Rapid development of new quantum technologies.



Our World
in Data

Transistor count

10.000.000.000

5.000.000.000

1.000.000.000

500.000.000

100.000.000

50.000.000

10.000.000

5.000.000

1.000.000

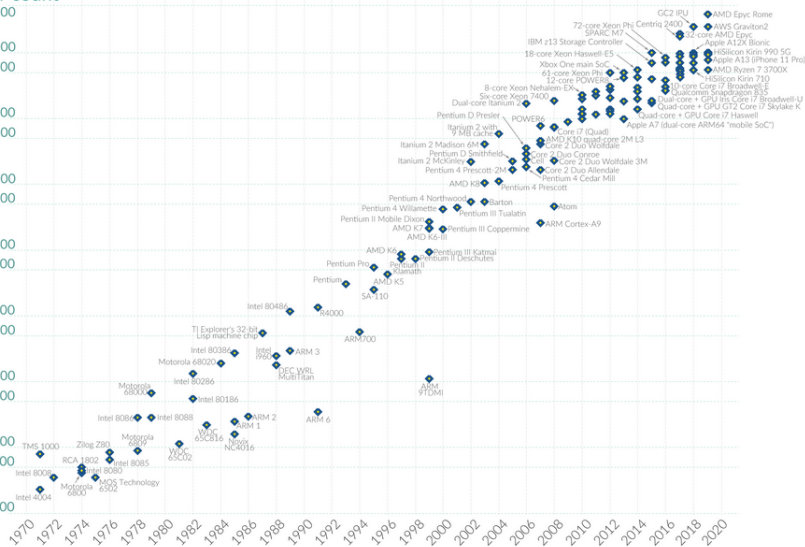
500.000

100,000

50 000

10,000

5.000



OurWorldinData.org – Research and data to make progress against the world's largest problems.

Licensed under CC-BY by the authors Hannah Ritchie and Max Roser.

MOSFET Process Node Evolution (1968–2027)

Year	Size
1968	20 μm
1971	10 μm
1974	6 μm
1977	3 μm
1981	1.5 μm
1984	1 μm
1987	800 nm
1990	600 nm

Year	Size
1993	350 nm
1996	250 nm
1999	180 nm
2001	130 nm
2003	90 nm
2005	65 nm
2007	45 nm
2009	32 nm

Year	Size
2010	28 nm
2012	22 nm
2014	14 nm
2016	10 nm
2018	7 nm
2020	5 nm
2022	3 nm
2025*	2 nm
2027*	1 nm

Motivation: Quantum Information Applications

- **Quantum Simulation:** Simulate quantum systems (too complex for classical computers)
 - **Chemistry:** molecular structure, reaction rates
 - **Material science:** high-temperature superconductors, exotic materials.
 - **Drug discovery:** modeling complex biomolecules and protein folding.
- **Quantum Cryptography**
 - **Quantum Key Distribution (QKD):** Securely exchange cryptographic keys using quantum states (e.g., BB84 protocol).
 - **Post-quantum cryptography:** Developing classical systems resistant to quantum attacks.
- **Quantum Metrology & Sensing:** Make ultra-precise measurements using quantum effects.
 - Timekeeping (atomic clocks).
 - Gravitational wave detection (e.g., LIGO).
 - Navigation systems (GPS alternatives).
 - Medical imaging and magnetic field sensors.

Motivation: Quantum Information Applications

- **Quantum Communication:** Transmit quantum states or information.
 - **Quantum Internet** (entanglement-based communication).
 - **Long-distance QKD** via quantum repeaters.
 - **Secure cloud quantum computing.**
- **Quantum Machine Learning (QML):** Accelerate ML algorithms using quantum computing advantages.
 - Faster optimization and sampling.
 - Quantum-enhanced pattern recognition.
 - Hybrid quantum-classical neural networks.
- **Quantum Algorithms:** Solve certain computational problems more efficiently than classical algorithms.
 - **Shor's algorithm:** Exponential speedup in factoring large integers (threatens RSA).
 - **Grover's algorithm:** Quadratic speedup for unstructured search problems.
 - **Quantum Fourier Transform (QFT):** Used in signal processing and cryptography.

Motivation: Quantum Information Applications

- **Financial Modeling:** Solve hard combinatorial problems faster.
 - Option pricing (quantum Monte Carlo).
 - Risk analysis and optimization.
 - Quantum-inspired algorithms for high-speed trading strategies.
- **Optimization Problems:** Solve hard combinatorial problems faster.
 - Logistics and supply chains.
 - Scheduling and routing.
 - Traffic flow optimization.
 - Energy grid management.
- **Fundamental Research:** Explore the foundations of physics and computation.
 - Study of quantum foundations (entanglement, non-locality, contextuality).
 - Reversible computing and thermodynamics of information.
 - Quantum complexity theory.

Summary of Quantum Applications

Domain	Applications	Impact
Quantum Simulation	Chemistry, physics, drug discovery	Scientific breakthroughs
Quantum Cryptography	QKD, secure communications	Unbreakable security
Quantum Metrology	Timekeeping, gravity sensing, EM field measurement	Precise instruments
Quantum Communication	Entanglement networks, quantum internet	Future of secure data transmission
Quantum Machine Learning	Speedup in learning and optimization	Smart and fast decision systems
Quantum Algorithms	Shor, Grover, QFT	Speedup in key tasks
Financial Modeling	Risk analysis, pricing, optimization	Better market strategies
Optimization Problems	Logistics, traffic, resource allocation	Efficient systems
Fundamental Research	Information theory, complexity, quantum foundations	Deeper theoretical understanding

Reminder:

Classical Information

Classical Computing

What is Classical Information?

- **Classical information is build from bits**
- Bits have symbolic values **0 or 1**
- **Information is Physical:** always encoded on physical phenomena:
 - *Voltage, Currents,*
 - *Charge,*
 - *Magnetization, etc.*

Classical Information is

- **Discrete** (either 0 or 1),
- **Deterministic** (predictable)
- **Copyable** (we can measure and copy it as many times as we like)

Bit Transformations: Logic Gates

- Logic gates transform bits using Boolean functions.
- Common gates: AND, OR, NOT, XOR, NAND, NOR.
- Most gates are **irreversible**, meaning inputs cannot be recovered from outputs \Rightarrow **classical computation destroys information**.
- Quantum Gates are Reversible (unitary) \Rightarrow preserve information.

Computation and Information Processing

- **Classical computation** = sequence of logic operations on bits.
- Information can be stored (memory), copied, erased.
- **Every bit that is erased during computation has an energy cost**
 $E = kT \ln 2$ (Landauer's Principle)
- **Error correction is needed in noisy environments.**

Error correction is the process of detecting and fixing errors in transmitted or stored data by **adding structured redundancy** \Rightarrow is a **clever way of encoding information** so that errors can be identified and corrected

Figure. 01

Basic Logic Gates with Truth Table

YES Gate



Boolean Expression: $Y = A$

Truth Table:

INPUT		OUTPUT (Y)
A		
0		0
1		1

NOT Gate

WWW.ETechnoG.COM



$$Y = A'$$

INPUT		OUTPUT (Y)
A		
0		1
1		0

INPUT		OUTPUT (Y)
A	B	
0	0	0
0	1	0
1	0	0
1	1	1

AND Gate



$$Y = A \cdot B$$

INPUT		OUTPUT (Y)
A	B	
0	0	1
0	1	1
1	0	1
1	1	0

NAND Gate



$$Y = \overline{A \cdot B}$$

OR Gate



$$Y = A + B$$

INPUT		OUTPUT (Y)
A	B	
0	0	0
0	1	1
1	0	1
1	1	1

NOR Gate



$$Y = \overline{A + B}$$

INPUT		OUTPUT (Y)
A	B	
0	0	1
0	1	0
1	0	0
1	1	0

XOR Gate



$$Y = A \oplus B$$

INPUT		OUTPUT (Y)
A	B	
0	0	0
0	1	1
1	0	1
1	1	0

INPUT		OUTPUT (Y)
A	B	
0	0	1
0	1	0
1	0	0
1	1	1

XNOR Gate



$$Y = \overline{A \oplus B}$$

Information Content

- **Measures the surprise of an outcome x :** $I(x) = -\log_2 p(x)$ [bit]
- Less probable events carry more information.

Shannon Entropy

- **Measures average uncertainty of a random variable:**
 $H(X) = -\sum p_i(x) \log_2 p_i(x)$ [bit].
- Entropy quantifies the average information content per message.
- Entropy $H(x) = 0$ for $p(x) = 0$ or 1 (know/predictable outcome)
- **Entropy is maximum** when $p_i = \frac{1}{2} \Rightarrow H_i = 1$ bit (max chaos).

Events with $p_i = \frac{1}{2}$ have maximum unpredictability. If e.g. $p = \frac{1}{4}$ we know that probability for the event to happen is smaller than not to happen!

Joint, Conditional Entropy and Mutual Information

- **Joint Entropy:** Uncertainty of (X, Y) ,
$$H(X, Y) = - \sum p(x, y) \log_2 p(x, y)$$
- **Conditional Entropy:** Uncertainty of Y given X ,
$$H(Y|X) = H(X, Y) - H(X)$$
- **Mutual Information:** Shared info between X and Y ,
$$I(X; Y) = H(X) - H(X|Y)$$

Channel Capacity and Data Compression

- **Channel Capacity:** Max info transfer rate: $C = \max_{p(x)} I(X; Y)$
- **Source Coding Theorem:** Minimum average bits per symbol = $H(X)$.
- Enables compression (ZIP, MP3) and sets communication limits.

Quantum Information

What is Quantum Information?

Quantum information studies how information is **stored, manipulated, and transmitted** using **Quantum Mechanics**.

- The basic unit is the **quantum bit** or **qubit** (a quantum generalization of the classical bit).
- Quantum information enables new possibilities in computation, communication, and sensing by utilizing the “weird laws” of quantum mechanics.

Feature	Classical Bit	Quantum Bit (Qubit)
States	0 or 1	Superposition: $\alpha 0\rangle + \beta 1\rangle$
Copying	Can be copied	No-cloning: cannot copy unknown states
Measurement	Reveals state deterministically	Collapses probabilistically
Operations	Boolean logic (often irreversible)	Reversible, unitary operations
Correlations	Statistical	Entanglement (non-local)

Quantum Mechanics of a Qubit

- In quantum mechanics, a physical system is described by a **state vector** in a **Hilbert space**.
- Hilbert space is a complex vector space with an inner product.
- A **qubit** is a two-level quantum system with basis states $|0\rangle$ and $|1\rangle$.
- The general state of a qubit is a **superposition**:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$$

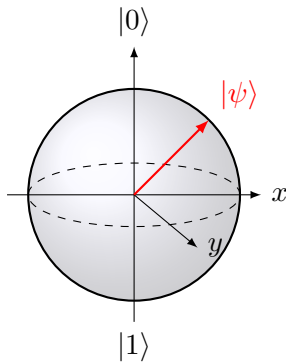
- Upon measurement, the qubit collapses to classical states $|0\rangle$ with probability $|\alpha|^2$ and to $|1\rangle$ with probability $|\beta|^2$.
- This leads to interference and phenomena unique to quantum systems.

Bloch Sphere Representation of a Qubit

- Any pure state of a single qubit can be written as:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right) |1\rangle$$

- Parameters $\theta \in [0, \pi]$, $\phi \in [0, 2\pi)$ define a point on the unit sphere.
- $|0\rangle$ and $|1\rangle$ are poles; superpositions lie on the surface.
- Visualization: **Bloch sphere**.



Physical Realizations of Qubits

- Qubits are implemented in various physical systems:
 - Superconducting circuits (Josephson junctions)
 - Trapped ions
 - Photonic qubits (polarization states)
 - Spins of electrons or nuclei
- All exploit two-level quantum systems.

Multiple Qubits and Entanglement

- Systems of multiple qubits form a joint Hilbert space via the tensor product.
- For 2 qubits: $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$
- Some quantum states **cannot be separated** into independent qubit states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- This phenomenon is called **entanglement**, and it leads to **non-classical, non-local correlations**.

*Quantum information theory is not just about building faster computers — it's about **redefining what information is** when nature is quantum.*

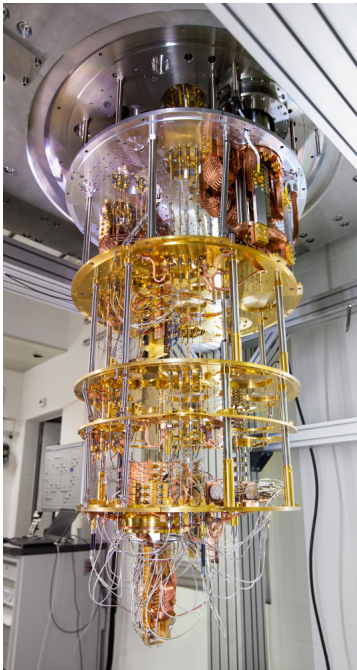
Key Quantum Phenomena

- **Superposition:** A qubit can be in a linear combination of state $|0\rangle$ and $|1\rangle$.
- **Entanglement:** Non-classical correlations between qubits.
- **Measurement:** Collapses quantum state to classical outcome (fundamentally probabilistic and irreversible).
- **No-Cloning:** Cannot duplicate an arbitrary unknown quantum state.
- **Unitary Evolution:** Quantum operations are reversible.
- **Decoherence and Quantum Noise:** Destroys superposition and quantum computation!

Why Quantum Information?

- **Quantum Computing:** Solve problems faster than classical computers.
- **Quantum Communication:** Secure information transfer via QKD.
- **Quantum Simulation:** Model complex quantum systems.
- **Quantum Sensing:** Ultra-precise measurements using quantum effects.

Quantum Computing



Quantum Computer

- Is a device that process quantum information.
- It uses quantum gates to process information
- Quantum effects like **superposition** and **entanglement** enable powerful computations.
- It works in cryogenic temperatures ($T \sim 1$ K) to lower noise and decoherence.

How Quantum Computing Works

- 1 **Qubits** represent quantum states in superposition.
- 2 **Quantum gates** manipulate the state vector of qubits.
- 3 **Quantum circuits** apply a sequence of gate operations.
- 4 **Measurement** collapses the quantum state to a classical result.

Example: $|\psi\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Aspect	Classical Computer	Quantum Computer
Unit of Info	Bit (0 or 1)	Qubit ($\alpha 0\rangle + \beta 1\rangle$)
Operations	Logic gates (e.g. AND, OR)	Unitary transformations (e.g. Hadamard, CNOT)
State Copying	Possible	No-cloning (cannot copy arbitrary state)
Correlations	Local	Non-local (Entanglement)
Measurement	Deterministic	Probabilistic collapse to 0 or 1

What Can Quantum Computers Do?

- **Shor's Algorithm:** Factor large numbers exponentially faster.
- **Grover's Algorithm:** Search an unstructured database in $O(\sqrt{N})$ time.
- **Quantum Simulation:** Model molecules, materials, and quantum systems.
- **Optimization and Machine Learning:** Speedups in specific structured problems.














Challenges of Quantum Computing

- Qubits are **fragile** — easily disturbed by noise and environment.
- Requires **low temperatures**, vacuum systems, and precise control.
- Needs **quantum error correction** to maintain reliable computation.
- Large-scale fault-tolerant quantum computers are still under development.

Why Quantum Computing Matters

- It's a new model of computation — not just faster, but **fundamentally different**.
- It helps us understand physics, optimize systems, and secure information.
- Quantum computing is an interdisciplinary field bridging physics, math, CS, and engineering.

Quantum Gates & Circuits

Operator	Gate(s)	Matrix
Pauli-X (X)	 	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

Quantum Gates

- Quantum Register is made of N-qubits, represented by a total wave function.
- Quantum gates are unitary linear operations ($U^\dagger U = I$) that are represented as a matrix

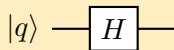
Quantum Gates

- Quantum Gates evolve quantum states without measurement.
- Act as building blocks of quantum circuits, analogous to logic gates.
- Qubits are represented in a vector form:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Example: Hadamard gate creates superposition

$$|0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{or} \quad |1\rangle \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$



Common Quantum Gates: Effect and Analogy

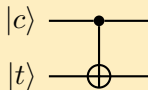
Gate	Symbol	Effect on Qubit	Classical Analog / Use
Pauli-X	X	Flips $ 0\rangle \leftrightarrow 1\rangle$	NOT gate (bit flip)
Pauli-Y	Y	Bit flip with added phase	No direct analog; combines X and Z
Pauli-Z	Z	Flips phase of $ 1\rangle$ (adds -1)	Phase inverter; no classical analog
Hadamard	H	Creates equal superposition from $ 0\rangle$ or $ 1\rangle$	No classical analog; key for quantum parallelism
Phase (S)	S	Adds a phase of $\pi/2$ to $ 1\rangle$	No classical analog; phase tracking
T ($\pi/8$)	T	Adds phase of $\pi/4$ to $ 1\rangle$	Used for universal quantum computation; no classical analog
CNOT	CX	Flips target qubit if control is $ 1\rangle$	Classical XOR (controlled-NOT)
Toffoli	CCX	Controlled-controlled-NOT (3-qubit gate)	Classical AND-controlled-NOT; universal reversible gate
SWAP	SWAP	Swaps two qubit states	Classical wire crossing or bit swap

Two-Qubit Gate: CNOT

- CNOT flips target qubit if control qubit is $|1\rangle$.

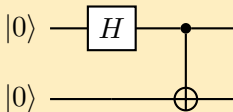
$$\text{CNOT} : |c\rangle |t\rangle \rightarrow |c\rangle |t \oplus c\rangle$$

- Essential for creating entanglement.

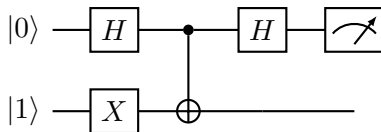


Example Quantum Circuit

- Combine gates to build algorithms.
- Example: create a Bell state.



Example: Deutsch Algorithm Circuit



- Solves the problem: Is a function $f : \{0, 1\} \rightarrow \{0, 1\}$ constant or balanced?
- Uses one query to f encoded in the oracle U_f .
- Demonstrates the power of quantum parallelism and interference.
- **Importance:** It is the simplest algorithm showing that a quantum computer can solve a problem with fewer queries than any classical deterministic algorithm.

Quantum Speedup: Why is it Powerful?

- Quantum computers leverage:
 - **Superposition**: Parallel evaluation of many states.
 - **Entanglement**: Correlation beyond classical limits.
 - **Interference**: Amplifying correct results, canceling wrong ones.
- Certain problems allow exponential speedup.

What Quantum Computers Excel At

- Quantum simulation of physical systems (chemistry, materials).
- Optimization problems (e.g., variational quantum eigensolvers).
- Cryptanalysis (e.g., breaking classical encryption).
- Machine learning subroutines (quantum kernels, data encoding).

Limits of Quantum Speedup

- Not all problems benefit from quantum acceleration.
- Quantum advantage depends on:
 - Problem structure (exploiting quantum parallelism).
 - Feasibility of coherent quantum operations.
- Classical algorithms remain superior for many practical tasks.

Decoherence & Noise

- Decoherence: loss of quantum information due to environment interactions.
- Types of noise:
 - **Amplitude damping (energy loss).**
 - **Phase damping (loss of coherence).**
 - Gate and measurement errors.
- Main challenge: **preserving coherence longer than computation time.**

Quantum Error Correction (QEC)

- Classical error correction: duplication of bits.
- Quantum: no-cloning, use entanglement & redundancy.
- Logical qubits encoded in multiple physical qubits.
- Detect & correct errors without measuring state directly.

Current Challenges in Hardware

- Scalability: Increasing qubit counts while maintaining fidelity.
- Error rates: Improving gate and measurement accuracy.
- Coherence time: Extending lifespan of qubit states.
- Integration of control electronics and cooling systems.

Quantum Hardware & Practicalities

Current State: NISQ Era

- NISQ: Noisy Intermediate-Scale Quantum devices.
- 50–1000 qubits, limited by noise and error rates.
- Useful for exploring near-term algorithms (e.g., VQE, QAOA).
- Not yet fault-tolerant.

Current Platforms & Players

- **IBM-Q Experience:** Cloud-based access to superconducting qubits.
- **Google Sycamore:** Quantum supremacy experiment (2019).
- **IonQ, Honeywell:** Trapped-ion quantum computers.
- **D-Wave:** Quantum annealing machines for optimization.

The Future of Quantum Computing

- Fault-tolerant, large-scale quantum processors.
- Quantum advantage in practical tasks (beyond supremacy demos).
- Integration with classical HPC systems.
- Potential paradigm shifts in cryptography, materials science, finance.

Hands-On Exploration

- Try quantum circuits on IBM Quantum Composer:
<https://quantum-computing.ibm.com/composer>
- Explore Qiskit (Python SDK for quantum computing).

Key Takeaways

- Classical computing reaches limits for certain problems.
- Quantum computing leverages superposition, entanglement, and interference.
- Quantum gates are unitary operations building quantum circuits.
- Algorithms like Grover's and Shor's demonstrate quantum speedup.
- Current devices (NISQ) are noisy, but evolving fast.

Quantum Computing in Perspective

- Not a replacement for classical computers — but a complement.
- Specialized in solving problems with inherent quantum structure.
- Engineering challenges: noise, scalability, error correction.
- Still an emerging field with significant theoretical & practical potential.

Exploring More

- Play with quantum circuits on IBM Quantum Composer
<https://quantum-computing.ibm.com/composer>
- Learn Qiskit: Python-based quantum computing SDK.
- Follow open-source resources: Qiskit Textbook, Quantum Algorithm Zoo.
- Stay updated with platforms like IBM, Google, IonQ.

Thank you!